Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

00101502.3

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 06/10/00
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 00101502.3

Anmeldetag:
Date of filing:
Date de dépôt: 26/01/00

Anmelder:
Applicant(s):
Demandeur(s):
EM Microelectronic-Marin SA
2074 Marin
SWITZERLAND

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Procédé pour tester un circuit intégré comportant des parties matérielles et/ou logicielles ayant un caractère de confidentialité

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
G01R31/317, G06F1/00

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Cas 1835
CM/cg

PROCEDE POUR TESTER UN CIRCUIT INTEGRE COMPORTANT DES PARTIES MATERIELLES ET/OU LOGICIELLES AYANT UN CARACTERE DE CONFIDENTIALITE

La présente invention est relative à des circuits intégrés contenant des parties matérielles et/ou logicielles présentant un caractère de confidentialité.

La fabrication de tout circuit intégré implique habituellement une procédure de test destinée à contrôler le bon fonctionnement de ses circuits matériels et le ou les logiciels qui y sont souvent mémorisés. Lorsque de telles parties matérielles et/ou logicielles sont confidentielles, il convient que cette procédure de test ne puisse les divulguer à des personnes non autorisées.

Le document US 5,039,850 décrit un circuit intégré de ce type qui contient lui-même son sous-programme de test. Il comporte une mémoire EEPROM destinée à contenir des informations secrètes dont un code d'identification du circuit intégré et des données confidentielles, par exemple.

Lorsqu'une procédure de test de ce circuit intégré doit être mise en œuvre, il est d'abord vérifié si le code secret a déjà été mémorisé. Si ce n'est pas le cas le sous-programme de test est exécuté sur tous les éléments non confidentiels du circuit. Si au contraire le code secret a déjà été mémorisé, le testeur doit envoyer le même code et s'il y a coïncidence entre celui-ci et le code mémorisé, la mémoire EEPROM est initialisée et les données confidentielles deviennent disponibles pour être exploitées par le circuit intégré. Cela veut dire que ces données restent confidentielles vis-à-vis du testeur, car un test ne peut être effectué que si le code secret n'est pas encore mémorisé. Cependant ceci signifie aussi qu'aucun test ne peut être appliqué à ces données confidentielles.

On comprend ainsi que le processus connu de cette antériorité vise uniquement le cas où le test est toujours effectué avant que les données confidentielles ne soient introduites dans le circuit intégré.

La présente invention a pour but de fournir un procédé de test de circuits intégrés par lequel un test peut être exécuté sur les parties confidentielles que contient le circuit sans que le contenu de ces parties devienne accessible à une personne non autorisée.

Elle a donc pour objet un procédé de test d'un circuit intégré contenant des éléments ayant un caractère de confidentialité à l'aide d'un testeur, présentant les caractéristiques définies dans la revendication 1.

Grâce à ces caractéristiques, le testeur peut avoir accès aux éléments à caractère confidentiel pour les tester, mais seulement s'il parvient à engendrer un mot de passe ayant une relation prédéterminée avec le mot de passe engendré dans le circuit intégré. L'accès aux éléments protégés est ainsi parfaitement préservé.

L'invention a également pour objet un circuit intégré présentant les caractéristiques de la revendication 7.

L'invention a encore pour objet un testeur présentant les caractéristiques de la revendication 11.

D'autres particularités de l'invention résultent des revendications dépendantes.

D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés sur lesquels :

- la figure 1 est un schéma simplifié d'un circuit intégré CI présentant des parties ayant un caractère de confidentialité, connecté à un testeur pendant que le procédé de l'invention est mis en œuvre;

- la figure 2 représente une partie du testeur pour illustrer une variante de l'invention.

Sur la figure 1, on a représenté un circuit intégré CI à tester ainsi qu'un testeur T. Lorsque le testeur T est branché sur le circuit CI ou sur un autre circuit intégré de même structure, l'ensemble permet de mettre en œuvre le mode d'exécution préféré de l'invention.

Le circuit intégré CI comprend une section 1 comportant des parties matérielles et/ou logicielles ayant un caractère de confidentialité et auxquelles l'accès est réservé. Il peut s'agir par exemple de mémoires ROM et/ou RAM contenant de l'information confidentielle telle que des algorithmes, des programmes, des données, ou des procédures de test de cette section confidentielle. Peuvent également faire partie de cette partie confidentielle une mémoire EEPROM dans laquelle sont enregistrés des paramètres de calibrage de modules électroniques de référence associés à des signatures correspondantes, des clés de chiffrement, des signatures de test etc. Il peut également s'agir de parties matérielles du circuit, comme les modules de référence tels qu'un oscillateur ou un régulateur de tension par exemple. Les spécialistes comprendront que la nature de l'information confidentielle ou celle des parties matérielles à protéger peut être quelconque, l'invention ayant

trait uniquement à un processus d'authentification permettant de tester la section confidentielle 1 du circuit CI.

La section confidentielle ou les parties confidentielles 1 sont accessibles pour être testées par l'intermédiaire d'une barrière 2 donnant aux parties 1 un accès conditionnel. Cette barrière 2 peut être matérialisée sous forme de deux multiplexeurs Mux 1 et Mux 2 connectés entre une interface d'entrée 3 du circuit CI et la section confidentielle 1. Le multiplexeur Mux 2 peut être commandé pour autoriser le passage des informations de test à partir de l'interface 3 par l'intermédiaire d'une connexion 3a et ce uniquement si un signal de commande est délivré par un comparateur 4 sur une connexion 4a.

La connexion 4a est reliée à la sortie du comparateur 4 dont les entrées sont reliées respectivement à des connexions 4b et 4c, cette dernière étant reliée à l'interface 3.

Le circuit CI comprend également un bloc de chiffrement 5 dans lequel peut être calculé un premier mot de passe G_k(RNG)-C à l'aide d'un algorithme de chiffrement. Celui-ci travaille avec un nombre aléatoire RNG-C engendré dans un générateur 6 de nombres aléatoires et avec une clé de chiffrement k mémorisée dans une section 7 d'une mémoire EEPROM. Le générateur 6 et la section de mémoire 7 sont donc connectés au bloc de chiffrement 5.

Ce dernier est également connecté par une sortie 8 de mot de passe à un registre de mot de passe 9 pour recevoir le premier mot de passe G_k(RNG)-C qui est par ailleurs relié à la connexion 4b vers le comparateur 4.

L'algorithme de chiffrement mis en œuvre dans le bloc de chiffrement 5 peut être un algorithme public connu en soi. Par exemple, il peut s'agir de l'algorithme standard connu sous le vocable DES par les spécialistes.

Le générateur de nombres aléatoires 6 est également relié à une interface de sortie 10 du circuit CI.

Le testeur T comprend une interface d'entrée 11 qui est connectée, lors d'un test, à l'interface de sortie 10 d'un circuit intégré CI à tester. Cette interface d'entrée 11 peut ainsi recevoir de ce dernier le nombre aléatoire RNG-C qui, au moment du branchement pour la réalisation d'un test, est présent dans le générateur de nombres aléatoires 6 du circuit CI.

Le testeur T comprend également un bloc de chiffrement 12 connecté à l'interface d'entrée 11 pour en recevoir le nombre aléatoire RNG-C engendré dans le circuit intégré CI. Ce bloc de chiffrement 12 est agencé pour effectuer un chiffrement à l'aide d'un algorithme identique à celui avec lequel travaille le bloc de chiffrement 5 du circuit CI. Le chiffrement dans le testeur T est

effectué à l'aide d'une clé de chiffrage k rangée dans une section 13 d'une mémoire EEPROM du testeur T. Cette clé k est la même que celle que contient la section de mémoire EEPROM 7 du circuit intégré CI.

Ainsi, le testeur T est capable de calculer un second mot de passe $G_k(RNG)$-T sur la base du nombre aléatoire RNG-C.

Le testeur T comprend également une interface de sortie 14 connectée à la sortie du bloc de chiffrement 12, afin que le mot de passe qui y est calculé puisse être acheminé vers le circuit intégré CI.

Cette interface de sortie 14 est également reliée à un bloc de test 15 capable de mettre en œuvre les fonctions de test auxquelles le circuit CI doit être soumis et dont les informations sont acheminées par l'intermédiaire des interfaces 14 et 3 vers le multiplexeur Mux 2 du circuit intégré CI.

Les interfaces 3, 10, 11 et 14 sont, de façon connue en soi, des "machines d'état" qui à l'aide des horloges internes respectives du circuit CI et du testeur T gèrent des protocoles d'émission et de réception d'acheminement des données entre les deux composants CI et T.

Le multiplexeur Mux 1 connecté en série en amont du multiplexeur Mux 2 vis-à-vis du testeur T, est connecté à l'interface 3 pour aiguiller les informations nécessaires à l'authentification vers les parties concernées du circuit telles que la section de mémoire EEPROM 7 et bloc de chiffrement 5 (pour simplifier les connexions correspondantes n'ont pas été représentées).

Ce premier multiplexeur Mux 1 est commandé ("ouvert") par un signal de mode de test transitant par un conducteur 16 en provenance du testeur T, tandis que le multiplexeur Mux 2 est commandé par la sortie du comparateur 4 (connexion 4a).

Les étapes essentielles de la procédure de test du circuit intégré CI se déroulent de la façon suivante.

Lorsque le testeur T est connecté au circuit intégré CI, la procédure de test est initiée par l'envoi du signal de mode de test passant sur le conducteur 16. Ceci provoque l'introduction dans le bloc de calcul 5 du nombre aléatoire RNG-C généré, à l'instant considéré, par le générateur 6 et de la clé k qui est extraite de la mémoire 7. Le premier mot de passe $G_k(RNG)$-C est alors calculé à l'aide de l'algorithme de chiffrement DES par exemple et ce mot de passe est placé dans le registre 9.

Le nombre aléatoire RNG-C est également envoyé vers le testeur T en étant acheminé par les interfaces 10 et 11 pour être appliqué au bloc de calcul 12 dans lequel est effectué également un calcul à l'aide du même

algorithme de chiffrement, à partir de la clé de chiffrement k extraite de la section de mémoire 13 et du nombre aléatoire RNG-C reçu. Ce calcul de chiffrement aboutira à la production d'un second mot de passe G_k(RNG)-T. Ce dernier est acheminé au circuit intégré CI par l'intermédiaire des interfaces 14 et 3 puis appliqué au comparateur 4.

Le comparateur 4 est agencé pour effectuer une comparaison bit à bit des deux mots de passe G_k(RNG)-C et G_k(RNG)-T qui lui sont appliqués.

S'il y a coïncidence entre les deux mots de passe appliqués au comparateur 4, cela voudra dire que l'authentification du testeur T a réussi et que ce dernier est donc habilité à avoir accès aux parties confidentielles 1. Le multiplexeur Mux 2 est commandé par le signal transitant sur la connexion 4a moyennant quoi la voie menant du testeur T aux parties confidentielles 1 du circuit intégré CI via la connexion 3a, est ouverte. Le testeur T peut alors accomplir les opérations de test requises par l'intermédiaire du bloc de test 15 pour vérifier les parties confidentielles 1 du circuit intégré CI quant à leur bon fonctionnement et si c'est le cas valider le circuit en question. A défaut d'une coïncidence, l'accès aux parties confidentielles 1 demeurera interdit au testeur T.

Afin d'augmenter la sécurité d'accès, et selon une première variante de l'invention illustrée en pointillés sur la figure 1, il est possible de n'autoriser le calcul du second mot de passe Gk(RNG)-T par le bloc de calcul 12 du testeur T qu'après vérification d'un troisième mot de passe préalablement calculé. A cet effet, avant le calcul du premier mot de passe G_k(RNG)-C dans le bloc de calcul 5 du circuit intégré CI, il est procédé au calcul d'un troisième mot de passe F_k(RNG)-C, calculé éventuellement sur un nombre de coups d'horloge différent de celui sur lequel est calculé le premier mot de passe G_k(RNG)-C.

Ce troisième mot de passe F_k(RNG)-C est envoyé au testeur T à la suite du nombre aléatoire RNG-C après initialisation de la procédure d'authentification, à travers les interfaces 10 et 11. Le bloc de calcul 12 du testeur T doit alors calculer également un quatrième mot de passe F_k(RNG)-T qui est appliqué à un comparateur 17 faisant partie du testeur T, ce comparateur étant connecté d'une part à l'interface 11 dont il reçoit le troisième mot de passe F_k(RNG)-C calculé dans le circuit intégré CI et d'autre part au bloc de calcul 12 pour en recevoir le quatrième mot de passe F_k(RNG)-T qui y est calculé.

Ce n'est que lorsque le comparateur 17 constate une coïncidence entre les troisième et quatrième mots de passe F_k(RNG)-C et F_k(RNG)-T qu'il envoie

au bloc de calcul 12 un signal d'autorisation de calcul du second mot de passe G_k(RNG)-T. A cet effet, le comparateur 17 est connecté par sa sortie à ce bloc de calcul 12.

Les fonctions F_k(RNG)-C et F_k(RNG)-T permettent d'authentifier le circuit intégré CI, tandis que les fonctions G_k(RNG)-C et G_k(RNG)-T permettent d'authentifier le testeur. Cette dernière partie constitue la partie importante de l'objet de l'invention, dans le but d'interdire à un testeur non autorisé d'accéder à des parties confidentielles du circuit intégré.

Selon une autre variante de l'invention qui est analogue à la variante venant d'être décrite et qui est représentée sur la figure 2, le troisième mot de passe F_k(RNG)-C est également calculé dans le circuit intégré CI comme précédemment décrit et acheminé au testeur T par l'intermédiaire des interfaces 10 et 11. Dans ce cas, ce troisième mot de passe est appliqué au bloc de calcul 12 qui est alors agencé pour effectuer un calcul sur ce mot à l'aide de l'algorithme inverse de celui utilisé pour le calcul du quatrième mot de passe F_k(RNG)-T. Ce calcul aura comme résultat un nombre aléatoire RNG-T qui est appliqué à un comparateur 17'. Celui-ci est à cet effet connecté par l'une de ses entrées au bloc de calcul 12, son autre entrée étant reliée à l'interface 11 pour recevoir RNG-C. La sortie du comparateur 17' est reliée au bloc de calcul 12 pour ne lui envoyer un signal d'autorisation de calcul du second mot de passe G_k(RNG)-T que si le comparateur 17' constate une coïncidence entre les nombres aléatoires RNG-C et RNG-T appliqués à ses entrées. Ce signal d'autorisation de calcul permet alors de déclencher le calcul du second mot de passe G_k(RNG)-T dans le bloc de calcul 12.

De préférence, lors de la fabrication du circuit intégré CI, les bits de la section de mémoire EEPROM 7 destinés à la mémorisation de la clé de chiffrement k sont tous portés à une valeur prédéterminée (par exemple tous les bits sont exclusivement formés de bits de niveau 0 ou exclusivement de bits de niveau 1). L'introduction de la clé de chiffrement dans cette section de mémoire 7 est effectuée dans une phase préliminaire aux tests pendant laquelle un contrôle de cohérence est effectué par l'intermédiaire d'un bloc de vérification de redondance 18 (Code redundancy check) que comprend la section de mémoire EEPROM 7. Le testeur T effectue cette opération qui, initialement, aboutit à un échec du fait des valeurs initiales des bits de mémorisation de la clé et de celle de la clé envoyée par principe différente. Le testeur T constatant que la clé n'est pas encore mémorisée, il en introduit une dans la section de mémoire EEPROM 7 après quoi l'emplacement

correspondant de la section de mémoire EEPROM 7 est bloqué en écriture et en lecture. La procédure de test telle que décrite ci-dessus peut alors commencer et se dérouler comme décrit ci-dessus.

Il est à noter que les mots de passe calculés dans le circuit intégré et le testeur et soumis aux comparaisons respectives n'ont pas nécessairement à être identiques. Il suffit qu'ils aient une relation prédéterminée entre eux qui sera vérifiée au cours de ces comparaisons. Le terme "coïncidence" doit donc être compris dans une acception large.

REVENDICATIONS

1. Procédé de test d'un circuit intégré (CI) contenant des parties matérielles et/ou logicielles (1) ayant un caractère de confidentialité, à l'aide d'un testeur (T), ce procédé étant caractérisé en ce qu'il consiste :

- dans ledit circuit intégré (CI) :

à engendrer un nombre aléatoire (RNG-C),

à chiffrer ce nombre aléatoire (RNG-C) à l'aide d'une clé (k) mémorisée dans le circuit intégré (CI) par l'intermédiaire d'un algorithme de chiffrement pour obtenir un premier mot de passe (G_k(RNG)-C) et

à envoyer le nombre aléatoire (RNG-C) vers ledit testeur (T),

- et, dans ledit testeur (T) :

à chiffrer parallèlement ledit nombre aléatoire (RNG-C) reçu à l'aide d'une clé (k) identique à celle utilisée dans ledit circuit intégré par l'intermédiaire d'un algorithme de chiffrement identique à celui mis en œuvre dans ledit circuit intégré (CI), pour engendrer un second mot de passe (G_k(RNG)-T), et

à envoyer ledit second mot de passe (G_k(RNG-T)) du testeur (T) vers ledit circuit intégré (CI),

- puis, dans ledit circuit intégré (CI),

à comparer lesdits premier (G_k(RNG)-C) et second (G_k(RNG)-T) mots de passe,

à libérer une voie de test (3a) menant dudit testeur auxdites parties à caractère confidentiel (1), seulement si la comparaison établit une coïncidence entre lesdits premier et second mots de passe (G_k(RNG)-C; G_k(RNG)-T), et

à effectuer le test desdits éléments à caractère confidentiel (1).

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste également :

- dans ledit circuit intégré (CI) :

à chiffrer ledit nombre aléatoire (RNG-C) à l'aide de ladite clé (k) mémorisée dans le circuit intégré (CI) par l'intermédiaire dudit algorithme de chiffrement pour obtenir un troisième mot de passe (F_k(RNG)-C);

à envoyer ledit troisième mot de passe (F_k(RNG)-C) audit testeur (T); et

- dans ledit testeur (T) :

à chiffrer ledit nombre aléatoire (RNG-C) reçu à l'aide de ladite clé (k) mémorisée dans ledit testeur par l'intermédiaire dudit algorithme de chiffrement pour obtenir un quatrième mot de passe (F_k(RNG)-T);

à comparer lesdits troisième et quatrième mots de passe (F_k(RNG)-C; F_k(RNG)-T); et

à autoriser le chiffrement dudit second mot de passe (G_k(RNG)-T) par ledit testeur (T) seulement s'il y a coïncidence entre lesdits troisième et quatrième mots de passe (F_k(RNG)-C; F_k(RNG)-T).

3. Procédé selon la revendication 1, caractérisé en ce qu'il consiste également :

- dans ledit circuit intégré (CI) :

à chiffrer ledit nombre aléatoire (RNG-C) à l'aide de ladite clé (k) mémorisée dans le circuit intégré (CI) par l'intermédiaire dudit algorithme de chiffrement pour obtenir un troisième mot de passe (F_k(RNG)-C);

à envoyer ledit troisième mot de passe (F_k(RNG)-C) audit testeur (T); et

- dans ledit testeur (T) :

à opérer le chiffrement inverse dudit troisième mot de passe reçu (F_k(RNG)-C), à l'aide de ladite clé (k) mémorisée dans ledit testeur (T) par l'intermédiaire dudit algorithme de chiffrement pour retrouver un nombre aléatoire calculé (RNG-T);

à comparer le nombre aléatoire (RNG-C) reçu dudit circuit intégré (CI) audit nombre aléatoire calculé (RNG-T); et

à autoriser le chiffrement dudit second mot de passe (G_k(RNG)-T) par ledit testeur (T) seulement s'il y a coïncidence entre lesdits nombres aléatoires reçu et calculé (RNG-T; RNG-T).

4. Procédé selon l'une des revendications 2 et 3, caractérisé en ce que le chiffrement desdits troisième et/ou quatrième mots de passe (F_k(RNG)-C; F_k(RNG)-T) étant réalisé sur la base d'un nombre de coups d'horloge différent de celui utilisé pour le chiffrement desdits premier et second mots de passe (G_k(RNG)-C; G_k(RNG)-T).

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce qu'il consiste, en ce qui concerne lesdites coïncidences, à vérifier l'égalité entre lesdits mots de passe (G_k(RNG)-C; G_k(RNG)-T) - (F_k(RNG)-C; F_k(RNG)-T) -, respectivement lesdits nombres aléatoires reçu et calculé (RNG; RNG-T).

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce qu'il consiste, à la fabrication dudit circuit intégré (CI), à mémoriser une valeur

prédéterminée de ladite clé de chiffrement, et lors de l'exécution de la procédure de test à l'aide dudit testeur (T), à envoyer audit circuit intégré (CI), une valeur de clé de chiffrement (k), à vérifier si ladite clé de chiffrement envoyée (k) présente la valeur prédéterminée mémorisée dans ledit circuit (CI), à commander la mémorisation de ladite clé envoyée dans ledit circuit (CI) au cas où une inégalité est constatée lors de ladite vérification et à bloquer dans ce cas la mémorisation dans ledit circuit (CI) de toute autre clé de chiffrement.

7. Circuit intégré (CI) comprenant des parties matérielles et/ou logicielles ayant un caractère de confidentialité (1) et des moyens (2, 3, 16) pour acheminer conditionnellement vers lesdites parties matérielles et/ou logicielles des informations de test, caractérisé en ce qu'il comprend :

- un générateur de nombres aléatoires (6);
- des moyens (7) pour mémoriser une clé de chiffrement (k);
- des moyens de calcul (12) pour, à l'aide d'un algorithme de chiffrement, calculer un premier mot de passe (G_k(RNG)-C) à partir de ladite clé et d'un nombre aléatoire engendré (RNG-C);
- des moyens (10) pour acheminer un nombre aléatoire (RNG-C) vers l'extérieur; et
- des moyens (4) pour comparer ledit premier mot de passe calculé (G_k(RNG-C) avec un second mot de passe reçu de l'extérieur (G_k(RNG-T), ledit second mot de passe étant calculé selon le nombre aléatoire engendré par le générateur, lesdits moyens de comparaison étant connectés auxdits moyens d'acheminement (2, 3, 16) de manière à ne les rendre transparents auxdites informations de test que s'ils constatent une coïncidence entre lesdits premier et second mots de passe (G_k(RNG)-C; G_k(RNG)-T).

8. Circuit intégré selon la revendication 7, caractérisé en ce qu'il comprend des moyens (9) pour mémoriser ledit premier mot de passe (G_k(RNG)-C) calculé, lesdits moyens de mémorisation étant placés avant les moyens de comparaison pour leur fournir ledit premier mot de passe mémorisé au moment de la comparaison avec le second mot de passe (G_k(RNG-T).

9. Circuit intégré selon la revendication 7, caractérisé en ce que les moyens de mémorisation de la clé de chiffrement sont une mémoire EEPROM qui comprend également un bloc de vérification de redondance.

10. Circuit intégré selon la revendication 7, caractérisé en ce que les moyens de calcul sont prévus pour calculer un troisième mot de passe

(F_k(RNG)-C) à l'aide de la clé de chiffrement, du nombre aléatoire engendré (RNG-C) et de l'algorithme de chiffrement du circuit, ledit troisième mot de passe étant destiné à être envoyé vers l'extérieur avec le nombre aléatoire à un testeur spécifique.

11. Testeur de circuits intégrés comprenant des parties matérielles et/ou logicielles ayant un caractère de confidentialité, ce testeur comportant des moyens (15) pour effectuer un test de bon fonctionnement desdites parties matérielles et/ou logicielles et des moyens pour acheminer les informations correspondantes audit circuit (CI), caractérisé en ce qu'il comprend :

- des moyens (11) pour recevoir un nombre aléatoire (RNG-C) engendré par un circuit intégré à tester;
- des moyens (13) pour mémoriser une clé de chiffrement (k); et
- des moyens de calcul (12) pour, à l'aide d'un algorithme de chiffrement, calculer un second mot de passe (G_k(RNG)-T) à partir de ladite clé de chiffrement (k) et du nombre aléatoire reçu (RNG-C);
- lesdits moyens de calcul (12) étant connectés auxdits moyens d'acheminement (14) pour envoyer ledit second mot de passe (G_k(RNG)-T) calculé audit circuit intégré (CI).

12. Testeur selon la revendication 11, caractérisé en ce que lesdits moyens de calcul (12) sont également agencés pour, à l'aide d'un algorithme de chiffrement, calculer un quatrième mot de passe (F_k(RNG)-T) à partir de ladite clé de chiffrement (k) et du nombre aléatoire reçu (RNG-C);

en ce que lesdits moyens (11) pour recevoir ledit nombre aléatoire sont également agencés pour recevoir un troisième mot de passe (F_k(RNG)-C) calculé dans ledit circuit intégré (CI), et

en ce qu'il comprend également des moyens de comparaison (17) pour vérifier la coïncidence entre ledit troisième mot de passe reçu (F_k(RNG)-C) et ledit quatrième mot de passe calculé (F_k(RNG)-T), lesdits moyens de calcul n'étant autorisé à calculer ledit second mot de passe (G_k(RNG)-T) que si les moyens de comparaison (17) constatent une coïncidence prédéterminée entre lesdits troisième et quatrième mots de passe.

13. Testeur selon la revendication 11, caractérisé en ce que :

- lesdits moyens (11) pour recevoir ledit nombre aléatoire sont également agencés pour recevoir un troisième mot de passe (F_k(RNG)-C) calculé dans ledit circuit intégré (CI), et

- lesdits moyens de calcul (12) sont également agencés pour, à l'aide d'un algorithme de chiffrement inverse, et à partir dudit troisième mot de passe (F_k(RNG)-C) calculé dans ledit circuit intégré (CI) et de ladite clé de chiffrement (k), recalculer un nombre aléatoire (RNG-T); et

en ce qu'il comprend également des moyens de comparaison (17') pour vérifier la coïncidence entre ledit nombre aléatoire reçu (RNG)-C) et ledit nombre aléatoire calculé (RNG-T), lesdits moyens de calcul n'étant autorisé à calculer ledit second mot de passe (G_k(RNG-T) que si les moyens de comparaison (17') constatent une coïncidence prédéterminée entre lesdits nombres aléatoires (RNG-C et RNG-T).

ABREGE

PROCEDE POUR TESTER UN CIRCUIT INTEGRE COMPORTANT DES PARTIES MATERIELLES ET/ OU LOGICIELLES AYANT UN CARACTERE DE CONFIDENTIALITE

Ce procédé utilise un testeur (T) susceptible d'être branché sur un circuit intégré (CI) à tester.

Un nombre aléatoire (RNG-C) est engendré et chiffré à l'aide d'une clé (k) par un algorithme de chiffrement pour obtenir un mot de passe (G_k(RNG)-C). Le nombre aléatoire (RNG-C) est envoyé vers le testeur (T) dans lequel on chiffre le nombre aléatoire (RNG-C) reçu à l'aide de la même clé (k) par un même algorithme de chiffrement pour y engendrer un second mot de passe (G_k(RNG)-T). Ce dernier est renvoyé vers le circuit intégré (CI) pour être comparé au premier mot de passe (G_k(RNG)-C). Le test des parties confidentielles (1) du circuit n'est autorisé que si les deux mots de passe présente la coïncidence requise.

Figure 1

1/ 1

Fig. 1

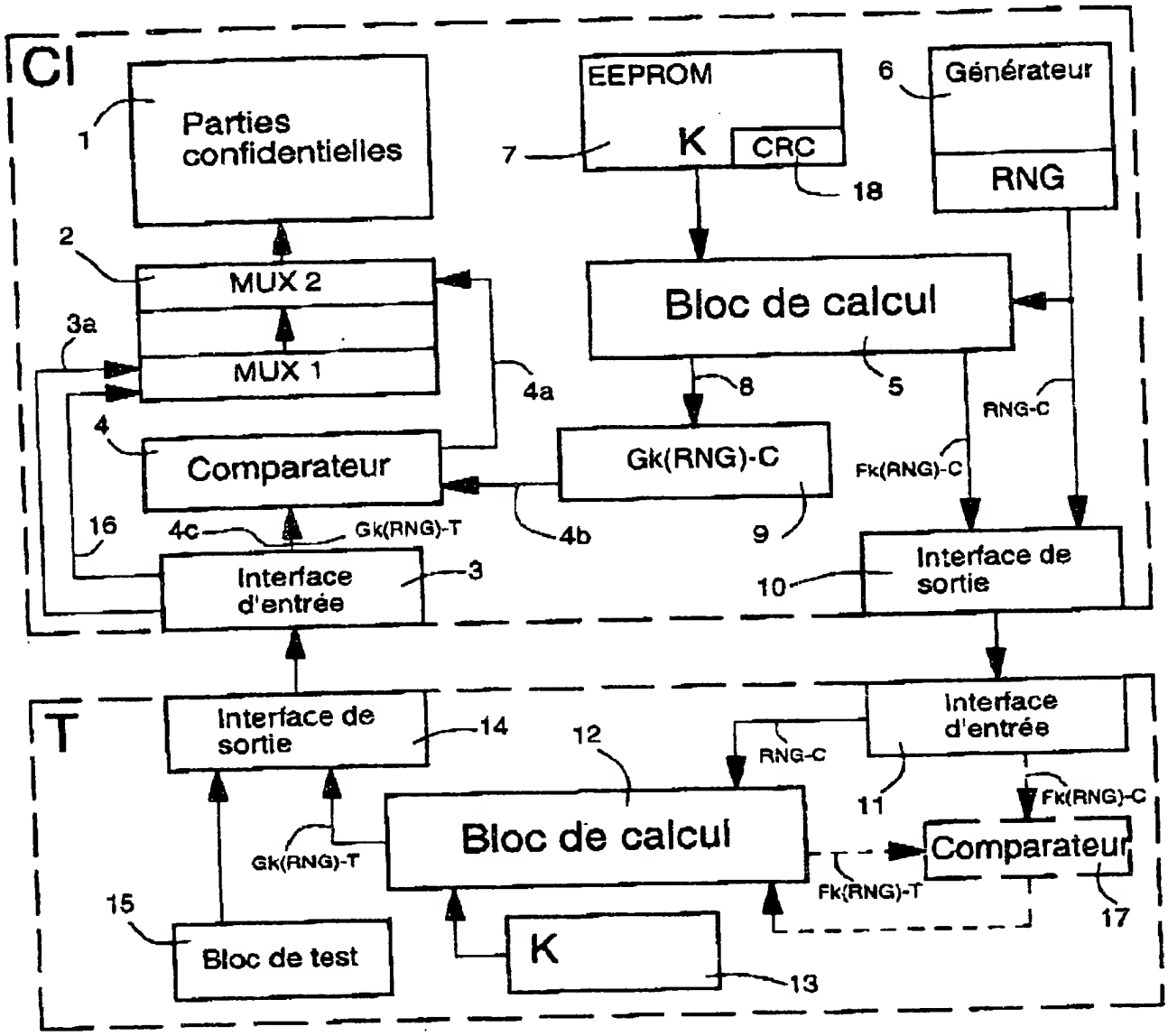
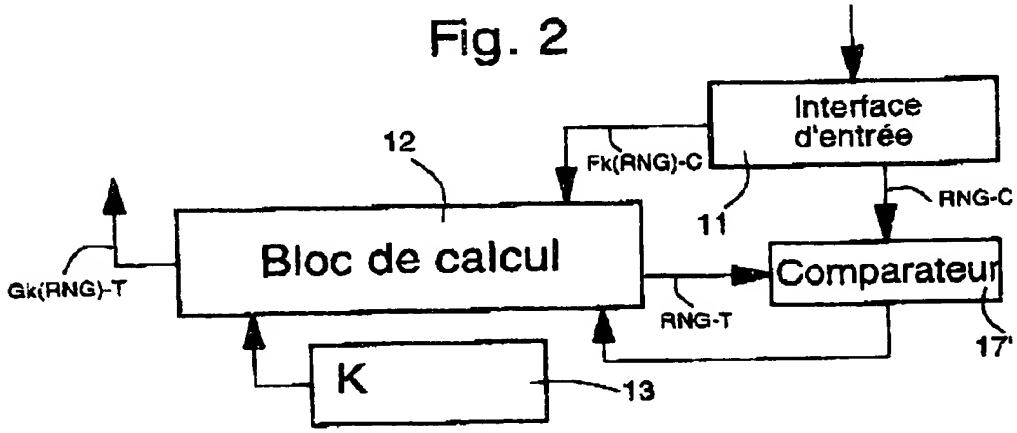

CI
Parties confidentielles
1
EEPROM
K
CRC
7
18
6
Générateur
RNG
2
MUX 2
MUX 1
3a
4a
Bloc de calcul
8
5
RNG-C
4
Comparateur
Gk(RNG)-C
Fk(RNG)-C
16
4c
Gk(RNG)-T
4b
9
Interface d'entrée
3
10
Interface de sortie
T
Interface de sortie
14
12
RNG-C
Interface d'entrée
11
Fk(RNG)-C
Gk(RNG)-T
Bloc de calcul
Comparateur
Fk(RNG)-T
17
15
Bloc de test
K
13

Fig. 2


Interface d'entrée
12
Fk(RNG)-C
RNG-C
11
Gk(RNG)-T
Bloc de calcul
Comparateur
RNG-T
17'
K
13

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.